УДК 681.3+681.031(043.2)

**Марченко В.А.**
*Институт кибернетики им. В.М. Глушкова, Киев*

## АТАКИ НА РАСПРЕДЕЛЕННЫЕ ВЕБ-ОРИЕНТИРОВАННЫЕ СИСТЕМЫ

Используемые современные сетевые технологии в основной своей массе обладают высокой сложностью и поэтому уязвимы для целенаправленных информационных атак. Причем такие атаки могут производиться удаленно, в том числе и из-за пределов национальных границ. Такие особенности ставят новые проблемы перед разработчиками и архитекторами телекоммуникационной инфраструктуры и информационных систем.

Трудность выявления проведения удалённой атаки и относительная простота проведения (из-за избыточной функциональности современных систем) выводит этот вид неправомерных действий на первое место по степени опасности и препятствует своевременному реагированию на осуществлённую угрозу, в результате чего у нарушителя увеличиваются шансы успешной реализации атаки.

В общем случаи считается что для того чтобы преодолеть систему защиты, достаточно взломать любой из ее компонентов. При этом если при создании подсистемы защиты для сложной информационной системы используются безопасные конструктивные блоки – это не гарантирует безопасность полученной системы защиты.

Современные информационные атаки по своему принципу функционирования и построения разделяются на две категории. Первая категория это информационные атаки, которые используют особенности архитектуры атакуемой системы или сервиса (особенности протоколов, реализации и взаимосвязи различных подсистем веб-сервиса и т.п.). Ко второй категории принадлежат атаки направленные на использование ошибок в реализации конкретной информационной системы. Частыми ошибками в некоторых системах является то, что они не гарантируют, уничтожения оригинальной информации после шифрования.

Существует множество известных атак их все можно разделить по сценарию их проведения на две схемы это атаки класса Man-In-The-Middle (MitM) и атаки класса Man-in-the-Browser (MitB).

Приведенные схемы могут применяться как для архитектурных атак, так и атак использующих ошибки реализации. Атаки, связанные с ошибками в реализации проще поддаются выявлению путем анализа и тестирования исходного кода системы, проведения нагрузочных испытаний и применяя различные методы оптимизации и верификации программных комплексов.

В этом докладе внимание уделяется особенностям атак на архитектуру информационной системы. Так как проактивное обнаружение подобных атак связаны с большими трудозатратами и с низкой эффективностью. То предлагается использовать анализ распространённых атак на веб-ориентированные системы с точки зрения эксплуатируемых схем проведения атак для выявления потенциальных слабостей в архитектуре реализуемой информационной системе.

*Научный руководитель – Н.И.Алишов, д.т.н., проф.*